



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,422	02/28/2002	Lauri Paatero	944-005.2	6221
4955 7590 04/02/2007 WARE FRESSOLA VAN DER SLUYS & ADOLPHSON, LLP BRADFORD GREEN, BUILDING 5 755 MAIN STREET, P O BOX 224 MONROE, CT 06468			EXAMINER SHIFERAW, ELEN I A	
			ART UNIT 2136	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	
3 MONTHS			04/02/2007	
			DELIVERY MODE PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/090,422	<b>Applicant(s)</b> PAATERO, LAURI	
	<b>Examiner</b> Eleni A. Shiferaw	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 21 December 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-57 and 60-67 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-57 and 60-67 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |                                                                                      |                                                                   |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____                                                          | 6) <input type="checkbox"/> Other: _____                          |

DETAILED ACTION

*Claim Status*

1. Independent claims 58-59 are cancelled.
2. Claims 66 and 67 are presently added.
3. Claims 1-57 and 60-67 are presented for examination.

*Response to Arguments*

4. Applicant's amendments and arguments with respect to amended independent claims 1, 29, 30, 60, and 65, newly added claims 66-67, and cancelled claims 58-59 have been considered but are moot in view of the new ground(s) of rejection.

*Claim Rejections - 35 USC § 103*

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-8, 10-11, 13-17, 19-21, 23-37, 39-40, 42-46, 48-50, 52-57, and 65- are rejected under 35 U.S.C. 103(a) as being unpatentable over Hayashi Seiichiro JP 09-261218 in view of Abburi et al. USPG PUBs 2003/0084306 A1.

Regarding claim 1, Seiichiro teaches a method/system comprising:

having an identity authenticated in a first system (0005; *computer 2 with authenticated certification*);

a second system causing a key to be generated for use in the second system (Abstract 5-6 and 0006; *computer 2 generates a public key A for the computer 2 and/or verification center 1*);

the second system generating a certificate for the key (0005, and 0010; *computer 2 generating certificate for the public key A*);

establishing the identity of the user in the second system by signing the certificate for the key using the authenticated identity of the user in the first system (Abstract, and 0010-0011; *computer 2 generating digital signature for the public key A using the authenticated identity of computer 2*).

Seiichiro fails to disclose wherein the certificate for the key for use in the second system contains one or more usage limitations, at least including a temporal limit on usage, and wherein the temporal limit requires that once a session on the second system is completed, the certificate or a corresponding key is destroyed. However, Abburi et al. discloses a user owning more than one device (fig. 25; user computing devices 1, 2, 3 or 1302a-c) and purchasing original licenses (1510a(1), 1510a(2), and 1510a(3)) to the first user computing device 1 and purchasing and using temporary licenses (1510a(1-3)b, and 1510b(4-6)b) to second/third user computing devices (par. **0452, 0024-0026, 0453-0436**; *near-term, decay, temporary licenses on second/third devices*); and temporary license provided on the second/third devices are terminated/decayed when the time session given to the second/third devices expire (par. **0455, 0463-0469, 0461, and 0452**) that reads on wherein the certificate for the key for use in the second system contains one or more usage limitations, at least including a temporal limit on usage, and wherein the temporal

limit requires that once a session on the second system is completed, the certificate or a corresponding key is destroyed.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Abburi et al. within the system of Seiichiro because they are analogous in generating a second temporary license to a second/third user devices based on user's first device identity (0420-0426 and fig. 25) and generating and/or verifying digital signature for second/third devices using asymmetric keys (0015-0018, and claim 1). One would have been motivated to incorporate the idea of Abburi et al. within the system of Seiichiro because it would control license usage on second/third user devices and would require the user making another payment upon expired second/third temporary license.

Regarding claims 29 and 65, Seiichiro teaches a method/program comprising:

generating a key for use in a network environment by a user having an authenticated identity not associated with said network environment (Abstract 5-6 and 0006; *computer 2 generates a public key A for the computer 2 and/or verification center 1*);

generating a certificate for the key (0005, and 0010; *computer 2 generating certificate for the public key A*); and

establishing the identity of the user in said network environment by signing the certificate for the key using the user's authenticated identity (Abstract, and 0010-0011; *computer 2 generating digital signature for the public key A using the authenticated identity of computer 2*).

Seiichiro fails to disclose wherein the certificate for the key for use in said network environment contains one or more usage limitations, at least including a temporal limit on usage, and wherein the temporal limit requires that once a session on the second system is completed, the certificate or a corresponding key is destroyed. However, Abburi et al. discloses a user owning more than one device (fig. 25; user computing devices 1, 2, 3 or 1302a-c) and purchasing original licenses (1510a(1), 1510a(2), and 1510a(3)) to the first user computing device 1 and purchasing and using temporary licenses (1510a(1-3)b, and 1510b(4-6)b) to second/third user computing devices (par. 0452, 0024-0026, 0453-0436; *near-term, decay, temporary licenses on second/third devices*); and temporary license provided on the second/third devices are terminated/decayed when the time session given to the second/third devices expire (par. 0455, 0463-0469, 0461, and 0452) that reads on wherein the certificate for the key for use in the second system contains one or more usage limitations, at least including a temporal limit on usage, and wherein the temporal limit requires that once a session on the second system is completed, the certificate or a corresponding key is destroyed.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Abburi et al. within the system of Seiichiro because they are analogous in generating a second temporary license to a second/third user devices based on user's first device identity (0420-0426 and fig. 25) and generating and/or verifying digital signature for second/third devices using asymmetric keys (0015-0018, and claim 1). One would have been motivated to incorporate the idea of Abburi et al. within the system of Seiichiro because it would control license usage on second/third user devices and would require the user making another payment upon expired second/third temporary license.

Regarding claim 30 Seiichiro teaches a system comprising:

a device forming part of a second system, the device having means for causing a key to be generated for use in the second system by a user having an authenticated identity in a first system (abstract and par. 0006);

said device of the second system having means for generating a certificate for the key (0005, and 0010; *computer 2 generating certificate for the public key A*); and

a second device forming part of the first system, the second device having means for storing information regarding the authenticated identity of the user in the first system (0009-0011),

said second device further having means for communicating said information (0010-0011); and

wherein the device of the second system has means for receipt of said information from the second device (abstract lines 13-14), and further has means for establishing the identity of the user in the second system by signing the certificate for the key using the authenticated identity of the user in the first system (Abstract, and 0010-0011; *computer 2 generating digital signature for the public key A using the authenticated identity of computer 2*).

Seiichiro fails to disclose wherein the certificate for the key for use in the second system contains one or more usage limitations, at least including a temporal limit on usage, and wherein the temporal limit requires that once a session on the second system is completed, the certificate or a corresponding key is destroyed. However, Abburi et al. discloses a user owning more than

Art Unit: 2136

one device (fig. 25; user computing devices 1, 2, 3 or 1302a-c) and purchasing original licenses (1510a(1), 1510a(2), and 1510a(3)) to the first user computing device 1 and purchasing and using temporary licenses (1510a(1-3)b, and 1510b(4-6)b) to second/third user computing devices (par. **0452, 0024-0026, 0453-0436**; *near-term, decay, temporary licenses on second/third devices*); and temporary license provided on the second/third devices are terminated/decayed when the time session given to the second/third devices expire (par. **0455, 0463-0469, 0461, and 0452**) that reads on wherein the certificate for the key for use in the second system contains one or more usage limitations, at least including a temporal limit on usage, and wherein the temporal limit requires that once a session on the second system is completed, the certificate or a corresponding key is destroyed.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Abburi et al. within the system of Seiichiro because they are analogous in generating a second temporary license to a second/third user devices based on user's first device identity (0420-0426 and fig. 25) and generating and/or verifying digital signature for second/third devices using asymmetric keys (0015-0018, and claim 1). One would have been motivated to incorporate the idea of Abburi et al. within the system of Seiichiro because it would control license usage on second/third user devices and would require the user making another payment upon expired second/third temporary license.

Regarding claims 2, 31, and 32, Seiichiro teaches a method/system/apparatus, wherein the key is generated by the second system (Abstract lines 5-6 and 0006; *computer 2 generates a public key A for the computer 2*).



Regarding claim 3, Seiichiro teaches a method, wherein the key is generated by the first system (Abstract lines 5-6 and 0006; *computer 2 generates a public key A for the computer 2*).

Regarding claims 4 and 33, Seiichiro teaches a method/system, further comprising the step of: a third party communicating with the user of the second system and verifying the user of the second system by the authenticated identity of the user of the first system (0012 and 0013 lines 6-7; *computer 3 and verification*).

Regarding claims 5 and 34, Seiichiro teaches a method/system, wherein the third party is a server (0015-0016).

Regarding claims 6 and 35, Seiichiro teaches a method/system, wherein the key comprises a private-public key pair and where the certificate includes the public key of the key pair (0013).

Regarding claims 7 and 36, Seiichiro teaches a method/system, wherein the certificate further includes an identity which is the same as the authenticated identity of the user of the first system (0005).

Regarding claims 8, 11, 14, 27, 37, 40, 43, and 56, Seiichiro teaches a method/system/apparatus, where the authenticated identity of the user in the first system comprises a private-public key pair and a certificate issued by a certification authority (0013), and where the signing of the

Art Unit: 2136

second system generated certificate is by hashing at least some data in the certificate to obtain a hash value (0014-0015), encrypting this hash value using the private key of the first system private-public key pair, and adding the encrypted hash value to the certificate (0011 lines 7-9).

Regarding claims 10, 13, 15-16, 39, 42, and 44-45, Seiichiro teaches a method/system/apparatus, wherein prior to signing the certificate for the key for use in the second system, the user of the first system obtains access to its private key by entry of a password (PIN) (The examiner takes an official notice on the first system requiring a password authentication prior/PIN to signing certificate because it would enhance security see, Bradley et al. Pub. No.: US 2002/0194219 A1 par. 0256-0263).

Regarding claims 17 and 46, Seiichiro teaches a method/system, wherein the certificate for the key includes the full certification tree for the key, said full certification tree including a certificate of the first system for the user of the first system (0005).

Regarding claims 19 and 48, Seiichiro teaches a method/system, wherein the second system a computer connected to the Internet (0007).

Regarding claims 20 and 49, Seiichiro teaches a method/system, wherein the second system uses a security protocol for establishing a secure session (0004-0009; authenticated and encrypted).

Regarding claims 23 and 52, Seiichiro teaches a method/system, wherein the wireless identity module contains a private key of the user of the first system and wherein a corresponding public

key of the user of the first system is certified by a certification authority (0005).

Regarding claims 21, 24, 50 and 53, the combination teaches a security protocol for encryption, decryption and authentication but does not specifically disclose session being a secure socket layer session and/or the security protocol being selected from the group consisting of transport layer security, Internet protocol security protocol, and secure socket layer. The examiner takes an official notice on these limitations as a well known (see Jardin USPN 6,681,327 B1 for secure socket layer and IP security) because it would make the session secure and protected.

As per claims 25 and 54, Abburi et al. teaches a method/system, wherein one usage limitation is that a third party of the second system should accept the key for use in the second system only for certain types of operations (fig. 25-26).

Regarding claims 26 and 55, Seiichiro teaches a method/system, wherein an accepted operation is the use of the key for use in the second system for encryption of data but not for signature verification (0013-0016).

Regarding claims 28 and 57, Seiichiro teaches a method/system, where the first and second users are the same entity (0005).

7. Claims 9, 12, 18, 22, 38, 41, 47, 51, 60-64, 66, and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hayashi Seiichiro JP 09-261218 and Abburi et al. USPG PUBs 2003/0084306 A1 and in view of Lauper et al. USPN 7,016,666 B2.

Regarding claims 60 and 66, Seiichiro teaches a device comprising:

means for storing information regarding an authenticated identity of a user in a first system associated with the device (0005; *computer 2 with authenticated certification*);

means for receipt of a certificate from a second device that is part of a second system, the certificate being for a key that is for use in the second system (abstract lines 13-14); and

means for establishing the identity of the user in the second system by signing the certificate using the authenticated identity of the user in the first system and transferring the signed certificate to the device of the second system (Abstract, and 0010-0011; *computer 2 generating digital signature for the public key A using the authenticated identity of computer 2*).

Seiichiro fails to disclose wherein the certificate for the key for use in the second system contains one or more usage limitations, at least including a temporal limit on usage, and wherein the temporal limit requires that once a session on the second system is completed, the certificate or a corresponding key is destroyed. However, Abburi et al. discloses a user owning more than one device (fig. 25; user computing devices 1, 2, 3 or 1302a-c) and purchasing original licenses (1510a(1), 1510a(2), and 1510a(3)) to the first user computing device 1 and purchasing and using temporary licenses (1510a(1-3)b, and 1510b(4-6)b) to second/third user computing devices (par. **0452, 0024-0026**, 0453-0436; *near-term, decay, temporary licenses on second/third devices*); and temporary license provided on the second/third devices are terminated/decayed when the time session given to the second/third devices expire (par. **0455, 0463-0469**, 0461, and 0452) that reads on wherein the certificate for the key for use in the second system contains one or more usage limitations, at least including a temporal limit on usage, and wherein the temporal

limit requires that once a session on the second system is completed, the certificate or a corresponding key is destroyed. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Abburi et al. within the system of Seiichiro because they are analogous in generating a second temporary license to a second/third user devices based on user's first device identity (0420-0426 and fig. 25) and generating and/or verifying digital signature for second/third devices using asymmetric keys (0015-0018, and claim 1). One would have been motivated to incorporate the idea of Abburi et al. within the system of Seiichiro because it would control license usage on second/third user devices and would require the user making another payment upon expired second/third temporary license.

Seiichiro and Abburi et al. fail to explicitly disclose a wireless device and a wireless device for storing information regarding an authenticated identity of a user in a first system associated with the device. However Lauper et al. discloses a wireless device (fig. 4) storing the mobile device's certificate in the wireless device module 14 and using the certificate (col. 4lines 53-59). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Lauper et al. within the combination system because they are analogous in verification. One would have been motivated to incorporate the teachings of Lauper et al. because it would work on mobile wireless devices.

Regarding claims 9, 12, 18, 22, 38, 41, 47, and 51, the Seiichiro teaches a method/system/apparatus, wherein the private key of the first system private-public key pair is

Art Unit: 2136

stored in a device identity module forming part of the second device (0009-0011). Seiichiro fails to disclose the device being a wireless device. However Lauper et al. discloses a wireless device (fig. 4) storing the mobile device's certificate in the wireless device module 14 and using the certificate (col. 4 lines 53-59). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Lauper et al. within the combination system because they are analogous in verification. One would have been motivated to incorporate the teachings of Lauper et al. because it would work on mobile wireless devices.

Regarding claims 61-62, Seiichiro teaches a method/system/apparatus, wherein the key is generated by the second system (Abstract lines 5-6 and 0006; *computer 2 generates a public key A for the computer 2*).

Regarding claim 63, Seiichiro teaches a method/system/apparatus, where the authenticated identity of the user in the first system comprises a private-public key pair and a certificate issued by a Certification Authority (0013), and where the signing of the second system generated certificate is by hashing at least some data in the certificate to obtain a hash value (0014-0015), encrypting this hash value using the private key of the first system private-public key pair, and adding the encrypted hash value to the certificate (0011 lines 7-9).

Regarding claim 64, the combination teaches a method/system/apparatus, wherein prior to signing the certificate for the key for use in the second system, the user of the first system

Art Unit: 2136

obtains access to its private key by entry of a password (PIN) (The examiner takes an official notice on the first system requiring a password authentication prior/PIN to signing certificate because it would enhance security see, Bradley et al. Pub. No.: US 2002/0194219 A1 par. 0256-0263).

Regarding claim 67 the combination teach all the subject matter as disclosed above. The examiner takes an official notice on a wireless device wherein the second device includes a generating module configured to generate the key to be used in said second system (see Faccin et al. USPG PUBs 2002/0118674 A1 abstract wherein the wireless mobile 30 generating Diffie Hellman keys) because it is well known to generate keys in a wireless devices at the time of the invention and would make it secure.

### *Conclusion*

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

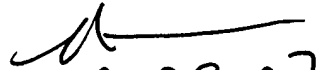
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



March 28, 2007

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
3,29,07